REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

This amendment changes claims in this application. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, is presented, with an appropriate defined status identifier.

Claims 7 and 17 have been amended. No new matter has been added.

After amending the claims as set forth above, claims 1-20 are now pending in this application.

Claim for Priority

The present application claims the benefit of the filing date of the foreign priority document, Japanese patent application no. 2000-009037, filed on January 18, 2000, and the right of priority provided in 35 U.S.C. § 119 is claimed. In support of this claim, applicant filed a certified copy of the original foreign priority document on January 17, 2001. Applicant respectfully requests that the Examiner acknowledge receipt of the certified copy of the foreign priority document in the next communication from the Patent Office.

Rejection under 35 U.S.C. § 102

Claims 1-20 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,867,578 to Brickell et al. (hereafter "Brickell"). Applicant respectfully traverses this rejection for at least the following reasons.

Claim 1 is directed to a signature calculation system by use of a mobile agent, and comprises a base host including "a partial signature auxiliary data generation means to which the random numbers generated by the random number generation means and a secret key of the owner of the mobile agent are inputted and which generates partial signature auxiliary data for distributing the information of the secret key of the owner of the mobile agent to the remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of the digital signature of the owner of the mobile agent are

calculated by remote hosts." Thus, in the structure of claim 1, random numbers and a secret key of the owner of the mobile agent are input into the partial signature auxiliary data generation means, and the partial signature auxiliary data generation means generates partial signature auxiliary data based on the random numbers and the secret key of the owner. The generated partial signature auxiliary data is for distributing the information of the secret key of the owner of the mobile agent to the remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of the digital signature of the owner of the mobile agent are calculated by remote hosts. Brickell fails to suggest at least this feature of claim 1.

Brickell discloses a multi-step digital signature system having a distributed root certifying authority (abstract). The system includes a distributed root certifying authority 20 which includes a set of RCA members 22-30 (Fig. 1, col. 5, lines 36-39). Each RCA member stores a private fragment (F_i) 88 of a root signature key (col. 8, lines 47-49). When signing a message, each RCA member separately applies its key fragment to the message without recombining the share to form a whole key (col. 7, lines 20-22). Each of the RCA members in a key generating group, RCA_{Bi}, selects a random number (x_{Bi}) between 1 and q-1 which is taken to be the private root key fragment for that member (col. 20, lines 22-26).

In contrast to claim 1, however, Brickell does not disclose a system including structure that allows a partial signature auxiliary data to be generated based on a generated random number and a secret key of an owner of a mobile agent, where the partial signature auxiliary data is distributed to remote hosts so that the partial signature auxiliary data will be used when partial signatures are necessary for calculation of a digital signature of the owner of the mobile agent are calculated by the remote hosts. In the Brickell system, the key fragments, (which the Office Action appears to equate with the partial signature auxiliary data as claimed) are not generated from a secret key of an owner of a mobile agent and a random number, but each key fragment is individually generated by an RCA member. Thus, Brickell does not anticipate claim 1.

Moreover, Brickell teaches away from the system as claimed in claim 1. Brickell specifically discloses that the root key never exists in a single location in whole form, but is

fragmented into shares (col. 7, lines 20-22). Thus, Brickell teaches away from a system where a whole secret key is used along with random numbers to generate partial signature auxiliary data, and the claimed system of claim 1 is not obvious over Brickell.

Independent claim 13 includes features similar to, or corresponding to, the features discussed above with respect to claim 1. Namely, claim 13 recites "a partial signature auxiliary data generation process for receiving the random numbers generated in the random number generation process and a secret key of the owner of the mobile agent as input data and generating partial signature auxiliary data for distributing the information of the secret key of the owner of the mobile agent to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are calculated by remote hosts." Thus claim 13 is patentable over Brickell for reasons analogous to claim 1.

Independent claims 14 and 18 are likewise patentable over Brickell. Claim 14 recites "a partial signature combining process for receiving one or more partial signatures calculated by one or more remote hosts as input data and outputting the digital signature calculated for the signature target data by use of a secret key of the owner of the mobile agent", while claim 18 recites "a partial signature combining process for receiving one or more partial signatures calculated by one or more remote hosts as input data and outputting the digital signature calculated for the signature target data by use of the newly generated secret key." Brickell fails to disclose or suggest at least the recited combining process of claims 14 and 18 which is based on a secret key of the owner of the mobile agent. Thus, claims 14 and 18 are patentable over Brickell.

Independent claims 7 and 17 are likewise patentable over Brickell. Claims 7 and 17 have been amended to respectively recite "a partial signature auxiliary data generation means to which the random numbers generated by the random number generation means are inputted, which generates a new secret key and a new public key corresponding to the newly generated secret key and generates partial signature auxiliary data for distributing the information of the newly generated secret key to the remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of the digital

signature of the owner of the mobile agent are calculated by remote hosts, and generating a digital signature for the partial signature auxiliary data using a secret key of the owner of the mobile agent" and "a partial signature auxiliary data generation process for receiving the random numbers generated in the random number generation process as input data, generating a new secret key and a new public key corresponding to the newly generated secret key, generating partial signature auxiliary data for distributing the information of the newly generated secret key to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are calculated by remote hosts, and generating a digital signature for the partial signature auxiliary data using a secret key of the owner of the mobile agent". Brickell fails to disclose at least generating a digital signature for the partial signature auxiliary data using a secret key of the owner of the mobile agent in the context of claims 14 or 17.

The dependent claims depend from one of the respective independent claims, and are patentable for at least the same reasons, as well as for further patentable features recited therein.

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date October 15, 2004 By Thomas G. Bilodeau

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

Thomas G. Bilodeau
Attorney for Applicant
Registration No. 43,438